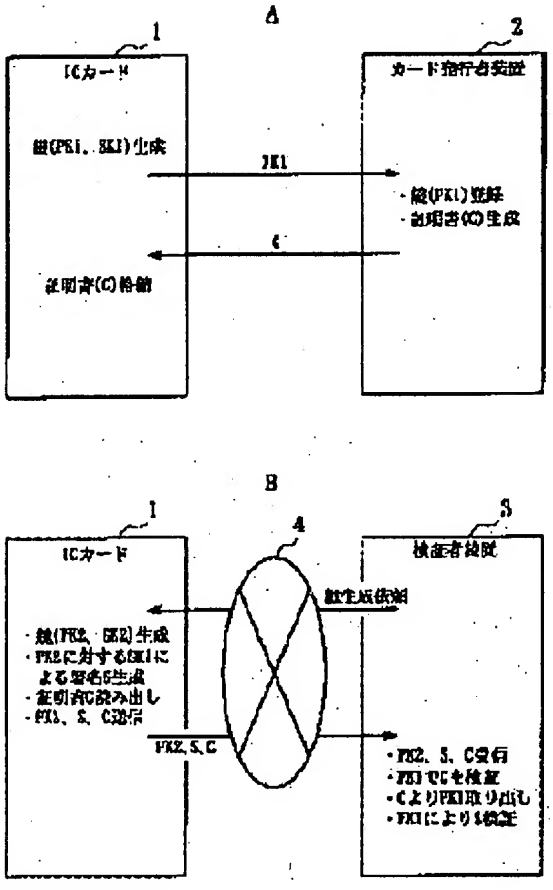
METHOD AND SYSTEM FOR GENERATING KEY FOR IC CARD

Publication number: JP2002300150
Publication date: 2002-10-11
Inventor: HIRATA SHINICHI; AKASHIKA HIDEKI
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
- international: ***B42D15/10; G06K19/07; G06K19/10; G09C1/00; H04L9/08; H04L9/10;*** **B42D15/10; G06K19/07; G06K19/10; G09C1/00; H04L9/08; H04L9/10;** (IPC1-7): H04L9/10; B42D15/10; G06K19/07; G06K19/10; G09C1/00; H04L9/08
- European:
Application number: JP20010094634 20010329
Priority number(s): JP20010094634 20010329

Abstract of **JP2002300150**

PROBLEM TO BE SOLVED: To solve the problem that it is impossible to confirm whether or not a key is surely generated in an IC card in the case that the key is generated online for the IC card via a network.
SOLUTION: First an IC card stores a secret key SK1 and a public key PK1, stores a public key certificate C generated by a credible 3rd party for the public key PK1, the IC card generates a new secret key SK2 and a new public key PK2 upon the receipt of a key generating command, uses the secret key SK1 corresponding to the public key PK1 of the public key certificate C to provide an electronic signature S to the newly generated public key PK2 and outputs the public key PK2 together with the public key certificate C. Verifying the public key certificate C and the electronic signature S can confirm that the newly generated public key PK2 is generated in the IC card.



FULL CONTENTS

[Claim(s)]

[Claim 1] An IC card stores the public key certification information generated by the 3rd person who can trust it to this public key while storing a secret key and a public key beforehand. The secret key corresponding to the public key of said public key certification information gives electronic signature to the public key which generated a new secret key and a new public key at the time of reception of a key generation command, and was newly generated, and it outputs with said public key certification information. The key generation method of the IC card characterized by the ability to check that the public key newly generated by verifying said public key certification information and said electronic signature is generated within an IC card.

[Claim 2] The IC card key generation method according to claim 1 characterized by including the signature candidate key algorithm version information, a serial number, a signer signature algorithm, Signer ID, the term of validity, and for [ID] a signature, a signature candidate key, and a signer signature in said public key certification information.

[Claim 3] A means by which an IC card stores the public key certification information generated by the 3rd person equipment reliable to this public key while storing the secret key and the public key, A means to answer a key generation command and to generate a new secret key and a new public key, A means to generate electronic signature with the secret key corresponding to the public key of said public key certification information, It has a means to give this electronic signature to the newly generated public key, and to output with said public key certification information. The key generative system of the IC card characterized by having a means by which the 3rd person equipment generates said public key certification information, and having a means to check that the public key by which verification person equipment verified said public key certification information and said electronic signature, and was newly generated is generated within an IC card.

[Claim 4] The key generative system of the IC card according to claim 3 characterized by including the signature candidate key algorithm version information, a serial number, a signer signature algorithm, Signer ID, the term of validity, and for [ID] a signature, a signature candidate key, and a signer signature in said public key certification information.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the key generation method of an IC card especially the method of generating on-line through a network, and a system.

[0002]

[Description of the Prior Art] As a new Information Storage Division medium which replaces a magnetic card in finance, communication, traffic, a public, the medical field, etc. in recent years Using the IC card which has big storage capacity by security top safety, two or more applications were carried in this, and the IC card system which provides two or more services has appeared. Moreover, what can download desired application if needed has appeared.

[0003] In such an IC card system, in order to attest the application in an IC card and a card, the code is used, at the time of issue, it stores or generates and the key for it is held. Moreover, in such an IC card system, generation

of a key new within an IC card at the time of online distribution of application and renewal of a key by online etc. is needed. Conventionally, this new key sends a key generation command to an IC card from card issuing person equipment or service provider equipment, and made it generate it within an IC card, for example, when it was a key of the public key cryptosystem, it made the secret key and the public key generate within an IC card, and it was outputting only public key information.

[0004]

[Problem to be solved by the invention] however, when key generation is performed on-line through a network to the IC card left distantly Since it cannot be checked whether surely the key generation has been performed within an IC card Neither distribution of just application nor the renewal of a key was guaranteed, for example, the inaccurate actor did **** of the IC card with the personal computer etc., the fake key was generated, and there was a problem which can receive distribution of application unjustly.

[0005]

[Means for solving problem] [the key generation method of the IC card of this invention / an IC card] while an IC card stores a secret key and a public key beforehand The public key certification information generated by the 3rd person who can trust it to this public key, for example, a card issuing person, is stored. The secret key corresponding to the public key of said public key certification information gives electronic signature to the public key which generated a new secret key and a new public key at the time of reception of a key generation command and was newly generated, and it outputs with said public key certification information. By verifying said public key certification information and said signature, it is characterized by the ability to check that the newly generated public key is generated within an IC card. [a generative system / an IC card] while the key generative system of the IC card of this invention stores a secret key and a public key A means to store the public key certification information generated by the 3rd person equipment reliable to this public key, A means to answer a key generation command and to generate a new secret key and a new public key, A means to generate electronic signature with the secret key corresponding to the public key of said public key certification information, It has a means to give this electronic signature to the newly generated public key, and to output with said public key certification information. It is characterized by having a means by which the 3rd person equipment generates said public key certification information, and having a means to check that the public key by which verification person equipment verified said public key certification information and said electronic signature, and was newly generated is generated within an IC card.

[0006]

[Mode for carrying out the invention] With reference to Drawings, the online IC card key generation method of this invention is hereafter explained per work example. Drawing 1 is the block diagram of the online IC card key generative system by this invention, drawing 2 A shows the procedure at the time of the card issuing of the online IC card key generation method of this invention, and drawing 2 B shows key generation and a verification procedure.

[0007] In the online IC card key generation method of this invention, as shown in drawing 2 A at the time of issue of IC card 1, IC card 1 sends only a public key to card issuing person equipment 2 while generating and storing the key for authentication (here, it is secret key SK1 and public key PK1) in the key generation section 11 in a card beforehand. In addition, this secret key SK1 and public key PK1 can also store in IC card 1 what card issuing person equipment generated. The certificate generation section 22 gives a signature of a card issuing person to public key PK1 sent, and card issuing person equipment 2 generates the certificate C proving this public key being just while registering public key PK1 to which the key registration section 21 has been sent. Public key PK1 of an IC card is enciphered with a publisher's secret key SKI, electronic signature is specifically generated, it attaches to public key PK1, the public key certification C of PK1 is generated, and this is sent to IC card 1. IC card 1 stores this in the certificate storing section 12.

[0008] Next, at the time of online distribution of application, or renewal of a key, as shown in drawing 2 B, verification person equipment (for example, service provider equipment) 3 sends a key generation command to IC card 1 through a network 4. IC card 1 is given to public key PK2 which answered this command, generated a new key (here, it is public key PK2 and secret key SK2) in the key generation section 11, generated the electronic signature S using secret key SK1 stored in the card in the signature generating section 13, and were newly generated. Public key PK2 specifically generated newly are enciphered by secret key SK1, and the electronic signature S is generated. Subsequently, Certificate C is read from the certificate storing section 12, and this certificate C is transmitted to verification person equipment 3 together with public key PK2 and the electronic

signature S which were newly generated. Verification person equipment 3 receives public key PK2 newly generated, the electronic signature S, and Certificate C, and the certificate verification section 31 verifies Certificate C and the electronic signature S. That is, Certificate C is decrypted with a publisher's public key PKI, registration public key PK1 of an IC card is taken out from Certificate C, and public key PK2 which decrypted the electronic signature S by this public key PK1 next, and were newly generated are taken out. Thus, surely public key PK2 verified by public key PK1 of IC card 1 proved to be just with Certificate C are generated by IC card 1.

[0009] In addition, although the public key certification which proves the justification of public key PK1 as public key certification information is used in the above-mentioned work example The signature candidate key algorithm version information, a serial number, a signer signature algorithm, Signer ID, the term of validity, and for [ID] a signature, a signature candidate key, and the thing proving a signer signature can be used as public key certification information.

[0010]

[Effect of the Invention] According to the method and equipment of this invention which were mentioned above, it can confirm that surely the key generated or updated on-line is generated in an IC card. Therefore, it becomes possible to perform key generation for online distribution of application, and renewal of a key by online.

[Brief Description of the Drawings]

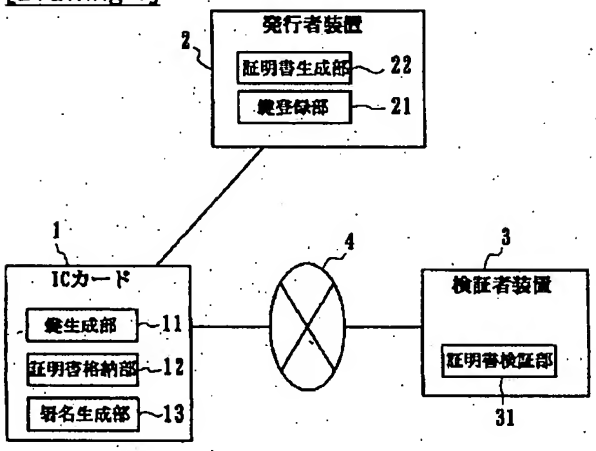
[Drawing 1] It is the block diagram of the online IC card key generative system by this invention.

[Drawing 2] A is the figure showing the procedure at the time of the card issuing of the online IC card key generation method of this invention, and B is the figure showing the procedure in key generation and verification.

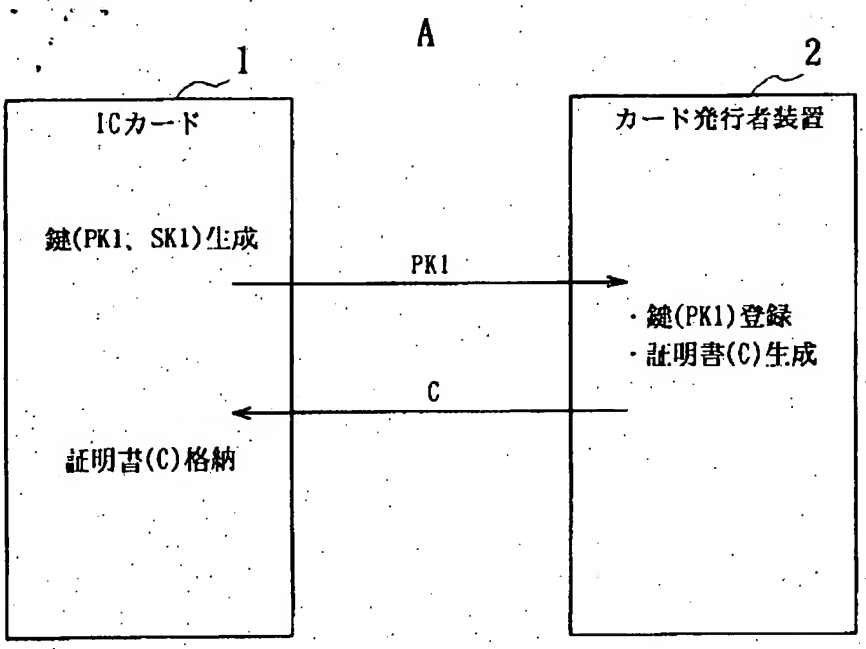
[Explanations of letters or numerals]

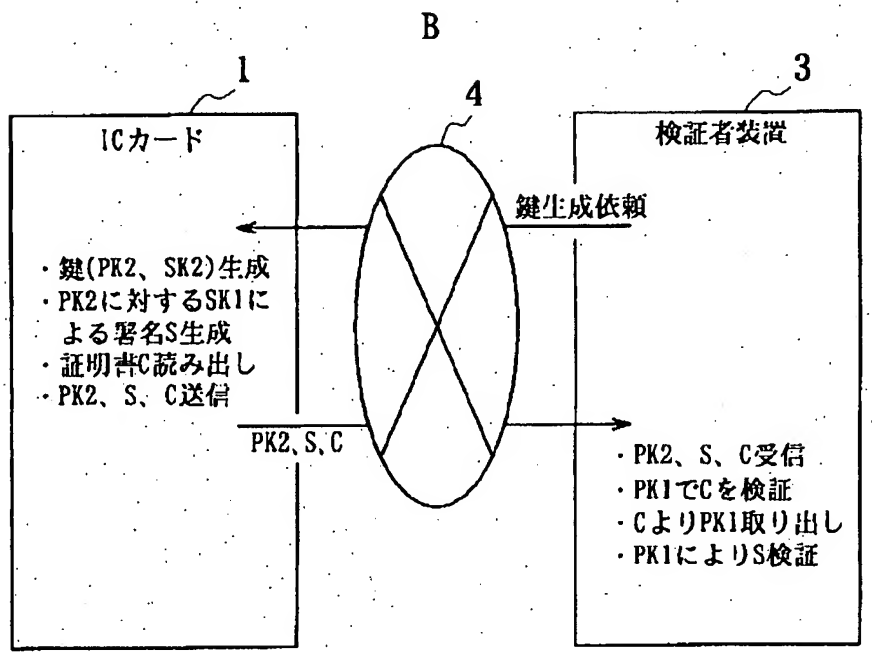
1 IC Card
2 Card Issuing Person Equipment
3 Verification Person Equipment
11 Key Generation Section
12 Certificate Storing Section
13 Signature Generating Section
21 Key Registration Section
22 Certificate Generation Section
31 Certificate Verification Section

[Drawing 1]



[Drawing 2]





[Translation done.]